

APPLICATION FOR UNITED STATES PATENT
FOR
METHOD FOR REMOTE ACCESS OF VEHICLE COMPONENTS

IN THE NAME OF

DAVID C. GELVIN
LEWIS D. GIROD
WILLIAM J. KAISER
FREDRIC NEWBERG
GREGORY J. POTTIE

FOR
SENSORIA CORPORATION

ATTORNEY DOCKET NO. 21200.716

Please direct communications to:

WILSON SONSINI GOODRICH & ROSATI
650 Page Mill Road
Palo Alto, CA. 94304
(650) 493-9300

Express Mail Number: EL473791031US

Method For Remote Access of Vehicle Components

RELATED APPLICATIONS

This application claims the benefit of United States Provisional Application
5 Number 60/158,013, filed October 06, 1999, United States Provisional Application
Number 60/170,865, filed December 15, 1999, United States Provisional
Application Number 60/208,397, filed May 30, 2000, United States Provisional
Application Number 60/210,296, filed June 08, 2000, United States Patent
Application Number (to be assigned-reference number 21200.702), filed October 04,
10 2000, United States Patent Application Number (to be assigned-reference number
21200.706), filed October 04, 2000, United States Patent Application Number (to be
assigned-reference number 21200.707), filed October 04, 2000, United States Patent
Application Number (to be assigned-reference number 21200.708), filed October 04,
2000, United States Patent Application Number (to be assigned-reference number
15 21200.709), filed October 04, 2000, United States Patent Application Number (to be
assigned-reference number 21200.710), filed October 04, 2000, United States Patent
Application Number (to be assigned-reference number 21200.711), filed October 04,
2000, United States Patent Application Number (to be assigned-reference number
21200.712), filed October 04, 2000, United States Patent Application Number (to be
20 assigned-reference number 21200.713), filed October 04, 2000, United States Patent
Application Number (to be assigned-reference number 21200.714), filed October 04,
2000, and United States Patent Application Number (to be assigned-reference
number 21200.715), filed October 04, 2000, all of which are incorporated by
reference.

25

GOVERNMENT LICENSE RIGHTS

The United States Government may have certain rights in some aspects of
the invention claimed herein, as the invention was made with United States

Government support under award/contract number DAAD16-99-C-1024 issued by US AMCAC NATICK Contracting Division.

BACKGROUND

5 Field of the Invention

This invention relates to the field of intelligent networks that include connection to the physical world. In particular, the invention relates to providing distributed network and Internet access to processors, controls, and devices in vehicles.

10 Description of Related Art

Typical modern vehicles include an information network within the vehicle, installed by the manufacturer. Many of the devices on this network are typically connected via a number of networks for different functions. In the near future it is expected that some of these functions will be consolidated so that a diverse set of 15 applications will use a common Original Equipment Manufacturer (OEM) bus. The Control Area Network (CAN) is a typical protocol used for such networks in the automotive industry. By this means, sensors, actuators, and computing elements for controlling the operations can all be linked in a common environment. This reduces the wiring within the vehicle, and allows for cost reduction in that the number of 20 different kinds of interfaces is vastly reduced. Because the OEM bus or functionally equivalent set of networks carries messages related to essential safety and security operations of the vehicle, only devices authenticated by the manufacturer can be added. In particular, the OEM bus needs to be guarded against devices that may cause congestion through repeated service requests, or malicious devices that issue 25 commands that may imperil vehicle operation or safety. Further, each manufacturer may potentially use different protocols on their own set of buses or proprietary buses. Consequently, it is costly to add consumer electronics to vehicles, or to perform upgrades of the information network.

In order to address some of the limitations of present-day vehicle information 30 networks, the Automotive Multimedia Interface Consortium (AMI-C) has developed

a set of common specifications for a multimedia interface to motor vehicle electronic systems. A particular aim is to accommodate a wide variety of consumer electronic and computer-based devices in the vehicle. The AMI-C standard network architecture, adopted by nearly all automobile manufacturers worldwide, reduces time to market and facilitates upgrades of vehicle electronics, supports deployment of telematics by providing standard interfaces, and reduces relative costs of electronic components. A variety of standards are being considered for AMI-C buses, among them IEEE 1394, MOST, and Intelligent Data Bus (IDB-C), with the possibility of multiple AMI-C approved buses within a vehicle.

10 Particular goals of the AMI-C forum are directed towards device interoperability, software interoperability, telematics support, logical security management, failsafe operation, and remote operation and service support. Device interoperability relates to the issue that consumer electronic devices and computer devices must interoperate with other systems installed in the vehicle, including communication, navigation, diagnostic and other systems.

15 Software interoperability relates to the issue that systems must support convenient, automatic discovery and initialization of software and hardware introduced into the vehicle by consumers, service organizations, or the vehicle manufacturer. Software portability, serviceability, and upgradeability are requirements within software interoperability.

20 Telematics support relates to the issue that voice and data communication must be provided for each of the installed devices or devices that may have been introduced into the passenger compartment. Logical security management relates to the issue that security services must be provided for access to vehicle data and systems. In particular, isolation must be provided between essential vehicle systems and any unauthorized local or remote access attempts.

25 Failsafe operation relates to the issue that some means for physical isolation between consumer and vehicle OEM bus must be provided. Thus, consumer electronics cannot be allowed to interfere in any way with the safe operation of the vehicle. Remote operation and service support relates to the issue that the network

system must provide remote access for authorized vehicle users and service providers.

While the goals of the AMI-C forum include desirable features, a standards body only issues requirements without providing means for solution. Beyond the 5 requirements expressed by the AMI-C forum, it is also desirable to have a complete, lasting solution for vehicle Internet access, with connectivity throughout the life cycle of the vehicle. Connectivity should begin in manufacturing and proceed through testing, distribution, sales, field use, maintenance, recall upgrade, and used vehicle sales. Desirable features of such a system include: connectivity available on 10 a national scale; connectivity to vehicles in all environments where the vehicle will be found using common hardware; connectivity in indoor and outdoor environments; and, scalability such that only a limited number of transactions are used for access to vast numbers of vehicles.

Further desirable features include: local information processing services at 15 the vehicle internetworking component that reduce the communication payload using reconfigurable systems; a single infrastructure solution for vehicle and Internet access over its life cycle; operation with a single national network service provider without the requirement of region-by-region negotiation with subscriber service providers; robust operation through atomic transaction methods to enable 20 deployment on vehicles using available power sources; secure operation that provides privacy and authentication; low component cost at both the vehicle node and the Internet access points; capability for rapid, low cost, after-market deployment of the connectivity solution; ability to deploy large (100 kb-100 Mb) data sets at a high speed and low cost; and, the use of standard web browsing tools 25 and database technology.

Network access to vehicles must be convenient and support mobility. Thus, wireless services are attractive. Conventional methods for wireless network access to vehicles include cellular telephony, cellular data packet delivery (CDPD) services, and satellite communication. Each of these conventional services requires 30 high subscription fees and high component costs. The RF transceivers used for

support of these networks must provide low bit error rates over long range links. This demands high performance systems and high transmitter power.

Consumer devices on an OEM or AMI-C bus could supply connectivity and Internet access solutions for cellular, CDPD, satellite communication, and other wireless services. While these services can be important components of the system, conventional network solutions present some limitations. For example, conventional systems are often not easily accessible on a national scale and, typically, only provide patchwork coverage. Conventional systems may require separate negotiations for service in each region.

10 Conventional services do not supply connectivity to vehicles in all environments. The conventional wireless services do not provide connectivity in typical assembly, maintenance, storage, and distribution environments at required latencies and costs. Different communications means are required for indoor and outdoor environments, without convenient linkage of these communications systems. Conventional services are not scalable such that only a limited number of transactions are required for access to vast numbers of vehicles. For example, a vast number of circuit switched calls must be placed on low rate channels. Local information processing services at the vehicle internetworking component that reduce required communication payload using reconfigurable systems are not 15 available in conventional systems.

20 Conventional services may require separate, regional negotiations for some services, which is a substantial obstacle to national or international deployment. Conventional services do not provide atomic transaction methods that verify completeness of transactions. For example, a cellular system will simply drop calls, 25 with the likelihood of requiring a fresh start on a bulk data transfer. The low power operation required for deployment on vehicles using, for example, available diagnostic port power sources is not compatible with conventional long range wireless communications. Secure operation that provides privacy and authentication is not available in conventional systems.

096306044000

Conventional long range wireless services require high component cost wireless devices, which is an obstacle to rapid, low cost, after-market deployment of the connectivity solution. Conventional systems lack the ability to deploy large (100 kb-100 Mb) data sets at low cost and at high speed.

5 Conventional means of self-assembly, while bringing a number of advantages, also have some limitations. For example, the Jini protocol is designed to enable assembly of functions on the Internet. It applies not to the original physical connection and assignment of internet protocol (IP) addresses, but rather to groups of users who are already connected and who desire particular services.

10 Requests are made to a central server, which downloads the appropriate software and enables set up of a session among scattered nodes. While the Jini protocol is heavy in the sense of demanding considerable memory and hardware support, it is robust over a variety of networks and extensive support software exists. Thus, while not a complete solution to the problem of self-assembly, it is desirable for a vehicle

15 network to be able to interact with Jini servers, and to support Jini for those devices with the capability of hosting its applications.

SUMMARY

A vehicle internetwork is provided comprising an information and control internetwork for vehicles, including hardware together with a suite of applications. The vehicle internetwork enables the secure and convenient addition of devices and software to a vehicle network. Among the functions supported are formation of subnetworks, authentication of new devices added to the network, bridging between heterogeneous networks, routing and security for multimedia traffic, and control of traffic based on priorities and security level. The vehicle internetwork permits secure operation of the internetwork and coupled devices in response to snooping, replay, denial of service, and unauthorized access attacks, with minimal intervention required by the vehicle operator or manufacturer. Further, mobile couplings to outside networks including the Internet are supported and, in contrast to conventional networking, most configuration takes place automatically and with no

intervention by a vehicle owner. A modular architecture enables distribution of functions, simplifying upgrades over the lifetime of the vehicle. Standard interfaces provide a universal socket, so that devices may be added irrespective of the make, model, or type of vehicle.

5 The descriptions provided herein are exemplary and explanatory and are intended to provide examples of the claimed invention.

BRIEF DESCRIPTION OF THE FIGURES

The accompanying figures illustrate embodiments of the claimed invention.

10 In the figures:

Figures 1 and 2 are a Wireless Integrated Network Sensor Next Generation (WINS NG) network architecture of an embodiment.

Figure 3 is a WINS vehicle internetwork architecture of an embodiment that provides scalable, secure, flexible, and low cost networking.

15 **Figure 4** is flow diagram of vehicle internetworking of an embodiment.

Figure 5 is a vehicular network architecture of an embodiment showing both internal and external couplings.

Figure 6 shows Mobile Internet Protocol (IP) (Mobile IP) connectivity using the WINS vehicle internetwork of an embodiment.

20 **Figure 7** shows the gateway functions of an embodiment linked or distributed using Internet Protocol (IP) techniques.

Figure 8 is a Serial Network Interface Connector (SNIC) and an associated internal proxy structure of an embodiment.

25 **Figure 9** is a Public Network Port (PNP) and an associated internal proxy structure of an embodiment.

Figure 10 is a WINS vehicle internetwork gateway of an embodiment.

Figure 11 is a port node architecture of an embodiment.

Figure 12 is a safety connector of an embodiment.

30 **Figure 13** shows a number of ways a WINS NG system of an embodiment can be reconfigured to accommodate different applications.

06600606-10C400

Figure 14 depicts a hybrid switch architecture of an embodiment.

Figure 15 is a port architecture of an embodiment.

Figure 16 is a vehicle internetwork application programming interface (API) structure of an embodiment.

5 **Figure 17** shows a gateway hardware and software interaction of an embodiment.

Figure 18 shows application programming interface (API) layering of an embodiment.

10 **Figure 19** shows default device discovery in a layered set of APIs of an embodiment.

Figure 20 shows Java/Jini application enablement in a layered set of APIs of an embodiment.

Figure 21 is a WINS vehicle internetwork of an embodiment.

Figure 22 is a WINS vehicle internetwork system of an embodiment.

15 **Figure 23** is a WINS vehicle internetworking system of an alternate embodiment.

DETAILED DESCRIPTION

The Wireless Integrated Network Sensor Next Generation (WINS NG) 20 sensors and nodes provide distributed network and Internet access to sensors, controls, and processors that are deeply embedded in equipment, facilities, and the environment. The WINS NG network is a new monitoring and control capability for applications in such sectors as transportation, manufacturing, health care, environmental monitoring, and safety and security. Wireless Integrated Network 25 Sensors combine microsensor technology, low power signal processing, low power computation, and low power, low cost wireless (and/or wired) networking capability in a compact system. The WINS NG networks provide sensing, local control, and embedded intelligent systems in structures, materials, and environments.

The WINS NG networks provide a more efficient means of connecting the 30 physical and computer worlds. Sensor nodes self-organize to form a network, and

seamlessly link to the Internet or other external network via a gateway node, which can be of the same type or different from the sensor nodes. The sensor nodes can themselves be of the same type or a variety of types. Network resources such as databases are available to the sensor network and the remote user through the

5 Internet or other external network.

The sensor nodes are constructed in a layered fashion, both with respect to signal processing and network protocols, to enable use of standard tools, ease real-time operating systems issues, promote adaptability to unknown environments, simplify reconfiguration, and enable lower-power, continuously vigilant operation.

10 High reliability access to remote WINS NG nodes and networks enables remote interrogation and control of the sensor network. This reliability is achieved using a plurality of couplings, with automatic adjustment of the processing and communications to deal with failures of any of these couplings. Linkage to databases enables extra resources to be brought to bear in analysis and archiving of

15 events, and database methods can be used to control the entire network in a more transparent manner, to enable more efficient control and design.

The WINS NG technology incorporates low-energy circuitry and components to provide secure communication that is robust against deliberate and unintentional interference, by means for example of new algorithms and antenna

20 designs. The network can further include distributed position location functionality that takes advantage of the communications and sensing components of the individual nodes, to simplify deployment and enable location of targets.

The sensor nodes can be of a variety of types, including very simple nodes that may, for example, serve as tags. These nodes can be constructed on flexible

25 polymer substrates, a material that may be used for a wide variety of synergistic uses. This construction results in more compact and capable systems, providing sensors, actuators, photo-cells and structural properties. Compact antennas for such packages have been developed. The network includes both wireless and wired communications capability, using a common protocol and automatically choosing

30 the more secure or lower power mode when it is available, providing more robust

and long-lived operation in potentially hostile environments. The network enables a wide variety of users with different data rate and power requirements to coexist as, for example, in wired or wireless mode vehicular applications. The flexibility of the design opens a wide variety of applications.

5 In another aspect, the layering of the WINS nodes with respect to processing and signal processing facilitates the rapid design of new applications. Layering further facilitates self-organization of complete applications, from network couplings through to interoperation with remote databases accessed through external networks such as the Internet. With this layering, the cost of deployment is radically 10 reduced even while remote operation is enabled.

15 **Figures 1 and 2** show embodiments of a WINS NG network. The network includes nodes 102, gateway nodes 104, server 106, and web assistants or node control web or browser pages (not shown), but is not so limited. The sensor nodes 102 include any combination of actuators, sensors, signal processors, energy or power supplies, data storage devices, wireless communication devices, wireline communication devices, and self-location capabilities. The sensor nodes 102 are distributed in an environment 199 that is to be monitored or controlled. The network can include heterogeneous elements. Local users 130 may interact, if authenticated, 20 with the network via the nodes 102 themselves through a local display and user interfaces (UIs). Non-local users can interact with the network through gateways 104. Thus, couplings to servers 106, database services 120, and other network resources are available, and user 132 can access the network with standard tools. The user or client computer can access the WINS network continuously or intermittently, and may interface via processors of vastly different capabilities 25 according to a particular application (e.g., personal computers, personal digital assistants (PDAs), or bidirectional pagers). A complete sensor network may, in one embodiment, be viewed as a distributed but active database that answers questions about the physical world, and acts upon the questions through the actuators. Multihop communication permits low power operation of dense WINS sensor 30 networks.

The network architecture of **Figures 1 and 2** is self-organizing with respect to an ability to distribute some combination of information and energy. The network interacts with remote users 132 and databases 120 when coupled to the Internet 110 or other networks using a gateway 104. The WINS node data is transferred over the 5 possibly asymmetric wireless link to an end user 132 or to a conventional wireless network service, for example an Internet Protocol (IP) network 110, through a WINS gateway 104 or a network bridge. Internetworking provides remote accessibility via web-based tools to data (e.g., signals and images), code (e.g., signal processing, decision support, and database elements), management (e.g., node and 10 network operation), and security functions.

The sensor nodes of an embodiment are remotely programmable. Furthermore, software is downloadable from storage locations in the sensor node network, or via the Internet from remote user locations or databases. Moreover, results or data products of sensor nodes may be remotely queried. Additionally, the 15 network is capable of supporting distributed processing and data storage functions in accordance with varying sensor node capabilities and application demands.

The WINS NG architecture readily accommodates the AMI-C goals. The WINS NG network includes a WINS NG gateway node and any number of other nodes that include a combination of sensing, signal processing, actuation, and 20 communications capabilities. The gateway couples to external networks such as the Internet. The network self-assembles, both with respect to establishment of the physical connectivity and in assembling applications. Through a set of open APIs, standard web browsers and database tools are used to control the operations of the network, request particular types of information, and archive the information of 25 interest. The gateway and other WINS NG nodes include as components the sensors and actuators, communications ports that support both wired and wireless communications, a real-time processor, and a higher level processor.

The WINS NG node and network architecture is well-suited for adaptation to and support of vehicular applications wherein, for example, a WINS NG gateway 30 functions to bridge the OEM and AMI-C buses while providing couplings with

09000000-0000-0000-0000-000000000000

external networks via at least one wireless port. Specifically, therefore, the WINS NG network includes a superset of the functions used in the core components of a vehicle internetwork. Thus, while WINS NG networks can include nodes with sensing, signal processing, and communications capabilities, the core network 5 components of vehicular networks may not use sensors, just as embodiments or configurations of the WINS NG gateway may not include sensors. However, the vehicle internetwork embodiments of the WINS NG technology do make use of the self-assembly, layered and open API set, separation of real-time and general purpose processing functions, and ease of connectivity to external networks and databases 10 characteristic of WINS NG networks. Consequently, the vehicle internetwork of an embodiment is regarded as a network including vehicle-specific configurations of WINS NG nodes.

The WINS vehicle internetwork of an embodiment provides an information and control internetwork for vehicles, including the associated hardware, together 15 with a suite of applications. An embodiment of the vehicle internetwork disclosed and claimed herein includes a wireline/wireless automotive gateway, programmable IDB-C bus interfaces, and complete internetworked vehicle systems. Automotive Multimedia Interface Consortium (AMI-C) network functions, including telematics, access to vehicle data systems, and security are enabled in this vehicle internetwork 20 using open interfaces that enable interaction with standard web-based software, tools, and databases. The vehicle internetwork leverages the development of hybrid wireless, wireline networked embedded systems, described in United States Provisional Application Number 60/158,013, filed October 06, 1999, United States Provisional Application Number 60/170,865, filed December 15, 1999, United 25 States Provisional Application Number 60/208,397, filed May 30, 2000, United States Provisional Application Number 60/210,296, filed June 08, 2000, United States Patent Application Number (to be assigned-reference number 21200.702), filed October 04, 2000, United States Patent Application Number (to be assigned-reference number 21200.706), filed October 04, 2000, United States Patent 30 Application Number (to be assigned-reference number 21200.707), filed October 04,

2000, United States Patent Application Number (to be assigned-reference number 21200.708), filed October 04, 2000, United States Patent Application Number (to be assigned-reference number 21200.709), filed October 04, 2000, United States Patent Application Number (to be assigned-reference number 21200.710), filed October 04, 5 United States Patent Application Number (to be assigned-reference number 21200.711), filed October 04, 2000, United States Patent Application Number (to be assigned-reference number 21200.712), filed October 04, 2000, United States Patent Application Number (to be assigned-reference number 21200.713), filed October 04, 10 2000, United States Patent Application Number (to be assigned-reference number 21200.714), filed October 04, 2000, and United States Patent Application Number (to be assigned-reference number 21200.715), filed October 04, 2000, and incorporated herein by reference.

Among the functions provided by the WINS vehicle internetwork of an embodiment are device and software interoperability, telematics support, 15 communication security and privacy, isolation of essential functions of the vehicle from consumer applications, remote operation, scalability, flexibility, open interfaces, support for local area wireless networks, accommodation of diverse device speeds on buses, and low cost. This vehicle internetwork further includes improved techniques: for enabling secure and convenient incorporation of diverse 20 devices and software; and, to resist denial of service, snooping, and replay attacks and unauthorized access to the network. A security architecture with security implemented at network ports and a proxy is also disclosed. This port and proxy 25 security architecture further enables simplified means for connecting both Internet Protocol (IP) capable and non-IP capable devices to the network, and permits convenient upgrades through addition of new devices throughout the lifetime of the vehicle.

The WINS vehicle internetwork can be used in a wide variety of 30 applications, including vehicle assembly, vehicle maintenance, fleet management, fleet reliability analysis, anti-theft systems, support for entertainment systems, coordination of vehicle systems with consumer electronics, and targeted advertising.

09680608-11004000

Among the advantages of the invention in enabling this broad range of vehicle reliability and consumer services are: its self-assembly and authentication from physical layer through to applications; application programming interfaces (APIs) that provide the ability to control physical parameters while using high-level and standard software tools; the separation of real time from non-real time processing; the proxy/port architecture; the integrated management of databases, CPU, internet access, and control (the network resources); and use of web tools and remote databases. These all contribute to low cost deployment and operation, and flexibility in the design of applications.

10

VEHICLE INTERNETWORKING ARCHITECTURE

Figure 3 is a WINS vehicle internetwork architecture 300 of an embodiment that provides scalable, secure, flexible, and low cost networking. While enabling the Automotive Multimedia Interface Consortium (AMI-C) network features, further services and features are enabled, as described herein. The WINS vehicle internetwork includes a gateway 302 that links external networks and the Original Equipment Manufacturer (OEM) 304 and AMI-C buses 306. The gateway 302 provides protocol translation, security, and privacy functions in bridging these networks, and can act as a network master for any of these networks as well as coordinate applications that span multiple networks.

The WINS vehicle internetwork gateway 302 is distinguished by the ability to control the flow of information between vehicle networks, and between these networks and external networks. Consequently, a separation is provided between the devices that communicate and those that control the communication. The port nodes 310 provide protocol translation for devices and networks connected to either bus 304 or 306, and additionally enable security functions to prevent unauthorized or misbehaving devices from disrupting the network.

Devices and functions supported on the OEM bus 304 through port nodes 310 include, but are not limited to, climate control, position location devices, Global Positioning System (GPS) devices, OBD-II port, cellular modems/embedded

processor, video/audio, multimedia players/embedded processor, sensor systems, switch clusters, and multiple device subnetworks. Devices and functions supported on the AMIC bus 306 through port nodes 310 include, but are not limited to, pagers, video/audio, multimedia players/embedded processor, personal digital assistants, and wireless local area network (LAN) ports.

This is but one example of the network topologies enabled by the WINS vehicle internetwork technology. For example, port nodes can bridge to subnetworks consisting of numerous devices like wired sensor/actuator systems such as WINS NG networks or devices, or wireless Bluetooth networks for consumer devices. Further, multiple gateways can be included to enable additional high speed networks to be overlaid. The WINS vehicle internetwork technology enables changes to the topology by means of its protocols for self-organization and its modular construction. This further extends to external networks. The APIs and protocols enable convenient coupling to external networks, and use of standard tools so that the network can be queried and, to some extent, controlled by authorized remote users.

Figure 4 is flow diagram of vehicle internetworking of an embodiment. A number of network elements including at least one node and at least one vehicle bus are coupled among at least one peripheral electronic device 402. Node information is manipulated, including configuration information and security information 404. In response to the node information, the network elements are automatically assembled and configured 406. Functions of the network elements are remotely controlled 408. Further, secure interoperability is provided among the network elements in response to the node information 410.

Figure 5 is a vehicular network architecture 500 of an embodiment showing both internal and external couplings. An automotive Internet Protocol (IP) router 502 is resident on the gateway, which serves to couple, for example, an IDB-C bus 504, 100 Base TX Ethernet 506, and an IEEE 1394 bus 508. Supported couplings to the Internet 599 include, but are not limited to, a Bluetooth modem 510, an IEEE 802.11 radio 512, and a mobile telephone 514. The Bluetooth 510 modem can

couple through a public network port (PNP) 520 to the IEEE 1394 bus 508, and in turn communicate with a personal digital assistant (PDA) 522 equipped with a Bluetooth radio. The latter may then couple to the Internet 599 through a service provider that specializes in low-rate communications, e.g., at the level of two-way paging.

The IEEE 802.11 radio 512 of an embodiment is coupled to the Ethernet network 506 to support communication with home or workplace networks 524 according to open services gateway initiative (OSGi) standards, which then have wired or wireless couplings to the Internet. A coupling that uses a mobile telephone 10 coupled to the IDB-C bus 504 can support an Internet coupling through a mobile telephone network.

The WINS vehicle internetwork of an embodiment includes functionality that enables convenient and secure coupling of diverse networks and devices. Consequently, each of the buses within the vehicle internetwork can support subnetworks. For example, a non-IP router supports an Ethernet or other coupling with on-board diagnostic (OBD), Audio Control Protocol (ACP), and LISA audio networks.

Software for managing the service discovery, device authentication, and other security features resides within the gateway or some other host such as a navigation computer. This software, or proxy, is coupled to the 100 Base TX Ethernet bus in an embodiment, but is not so limited. In alternate embodiments, the IP router, proxy, and non-IP router can be embedded within the gateway. Thus, through use of proxies and ports, such gateway functions can either be centralized or distributed within the network, while enabling secure network operation.

25 **Figure 6** shows Mobile Internet Protocol (IP) (Mobile IP) connectivity using
the WINS vehicle internetwork of an embodiment. The roaming vehicular network
602 can communicate using an 802.11 radio, a cellular radio, or a Bluetooth radio,
but is not so limited. Communication using the 802.11 radio is via a port to a home
network 604. Communication using the cellular radio is via a cellular network 606.
30 Communication using the Bluetooth radio is via a service station 608. Each of these

external entities are coupled to the Internet through networks including wired networks, wireless networks, and hybrid wired and wireless networks.

In operation, the vehicular network 602 tries to select the most cost-effective communication alternative that provides the desired level of service, but this can be problematic in that some alternatives only exist in certain places (e.g., home, or service station). Further, most alternatives will provide the automotive network with a different external address. The WINS vehicle internetwork solves this problem by having an internet service provider (ISP) assign a static IP address to the vehicle and a domain name server (DNS) mapping 610. For example, the ISP may look up the address in the location database (DB). Packets destined for the vehicle are sent to that static address. When the ISP receives a packet for the vehicle, it first checks its database to locate any potential addresses for the vehicle. The ISP tries to find a working address by pinging; if a working address is found, the ISP tunnels the packet to that address. Otherwise, the ISP uses the vehicle's cellular phone number to attempt to establish a coupling over the telephone network, and tunnel the packet through. While the cell phone network has the broadest geographic extent, it also has a higher associated cost, and thus the reason for attempting other means of communication. Potentially, any number of available methods of communication can be attempted.

Using network technologies that provide inexpensive short message service (e.g., two-way paging), the vehicle can periodically advertise its favored means of contact (i.e., cheapest and best method). Because of the costs of cellular telephony, there may need to be constraints on the use of the cellular phone connection. In some cases, the owner of the vehicle may want to be offline except when he specifically wants to dial out. Those skilled in the art will realize that there are numerous optimizations of mobile IP that are discussed in the networking research literature, for example, means intended to short-circuit the tunnel by sending directly to the vehicle's current address. The claimed invention is intended to encompass all such embodiments.

SECURITY

Proxy and port architecture

The large number of ways information can enter the vehicle internetwork, and the varied costs associated with the different external communication modes, 5 result in security issues including denial of service attacks, snooping and replay attacks, and unauthorized access. There can be both deliberate and unintentional denial of service attacks, in which the network or particular servers are flooded with data. This consumes scarce network resources and may even impair essential operations of the vehicle. Unintentional attacks are caused for example by 10 malfunctioning devices, or devices which were not designed to operate within the vehicle network.

Snooping and replay attacks are also of concern. An eavesdropper may see and replay confidential data such as passwords and control traffic related to vehicle security (e.g., doorlocks) to gain access to the vehicle system. Information can also 15 be gleaned from apparently public data, in the form of traffic analysis, so that usage patterns for services can be discovered or other information the consumer may wish to protect is compromised. There may also be attacks on personal privacy, for example, where control of a Bluetooth web camera or hands-free microphone system is seized.

20 Unauthorized access is also problematic. Access to applications can reduce utility for the intended users, and personal data can be compromised. Additionally, it is desirable to limit access to networking and routing resources only according to specified levels, as some of these resources may be in high demand (e.g., the IDB-C bus) while others may result in large connection charges (e.g., the cell phone).

25 While the standard interfaces associated with the AMI-C bus provide for ease of integration of diverse devices into the network, they have an associated risk that unauthorized devices may be added to the network which then issue commands that damage the operation of the network or vehicle. Thus, security measures are provided in an embodiment that: enable only authorized devices to be added; and, 30 accept only certain commands from particular classes of devices. These security

measures are provided in an embodiment without the need for significant modification of the integrated device in order to prevent the manufacturers of integrated products from incurring unnecessary expense. Instead, this burden largely falls upon the gateway, the port nodes, and an easy to use interface provided to the vehicle operator. As an example, while there is now a standard ISO/CD 5 15764 for authenticating devices to go into automobiles, the registration process is both costly and time-consuming, thereby placing great demand on consumers.

A security architecture of an embodiment implements security functions both at ports to the network (e.g., different varieties of port nodes such as PNPs, and 10 serial network interface connectors) and internally in a proxy that is hosted in the gateway or in some other host like the navigation computer or auto personal computer (PC). These can be regarded as complementary approaches to security, corresponding respectively to security at the access points to the network and 15 internal security. While in principle for entirely new networks it may be possible to have all security functions embedded in the ports (e.g., homogeneous WINS NG networks), in practice vehicular networks will include many legacy applications with 20 insecure protocols, and a second layer of security may be used to have the necessary degree of protection. At the same time, relying solely on internal security techniques makes it essentially impossible to resist denial of service of attacks due to malfunctioning devices; it is necessary in such cases to be able to physically shut off access.

A denial of service attack is handled in the network of an embodiment by having the network turn off an untrusted port at the connector, and block specific 25 applications at the connector that have not been authorized. Consequently, the port in collaboration with the proxy acts to quickly end such attacks. By blocking unauthorized applications at the connector, the gateway does not require the ability 30 to filter commands passing from one internal network to another, while it may exercise an ability to perform network intrusion detection.

Snooping and traffic analysis can be dealt with using techniques such as confounder codes and encryption that can be employed in applications that, in

09630608-1400400

providing security, assume the bus is insecure. However, a number of legacy applications may use insecure protocols, and device resource constraints may make security too expensive. The network of an embodiment reduces connector promiscuity by permitting only trusted devices such as the connectors described

5 herein to directly couple to the bus. These devices in turn act as bridges or switches, copying traffic only for the client, rather than exposing the client to all bus traffic. By this means, the chances of eavesdropping can be greatly diminished. It is thus not necessary in such instances for all data to and from the public Internet to be encrypted, since the application will determine the need. The proxy serves as the

10 single point of control for access to the external Internet, thus limiting access to only those users who are authorized. Access to internal services is similarly defined by a security policy, with the proxy or other devices authorized by the proxy serving to control access. For legacy controls that cannot support secure interfaces, proxy stubs are employed. Additionally, legacy applications may be filtered at the

15 connectors to internal and external networks to ensure data privacy and resist traffic analysis attacks.

Figure 7 shows the gateway functions of an embodiment linked or distributed using Internet Protocol (IP) techniques. The network uses IP to enable continued use of legacy systems, provide security, and provide flexibility of

20 implementation, but is not so limited. The IP router 702 routes between IP networks that run a variety of link and physical layers. Link interfaces 704 implement the link and physical layers. Internet Protocol packets from the router are encapsulated in link layer packets with the appropriate destination addresses, resolved by ARP (Address Resolution Protocol). The link interfaces 704 have input and output

25 buffers. Routing is performed based on the incoming interface and the destination IP address of an incoming packet, by selecting an outgoing interface for each packet.

On bootup, the router 702 detects the networks that attach to it and assigns addresses to them. Nodes on those networks get their addresses via the dynamic host configuration protocol (DHCP) 706. For this purpose, the router 702 provides a

30 minimal DHCP service to supply host and gateway addresses, and the address of the

“proxy” 708. The proxy 708 is a device that centrally manages the network and is responsible for security. It may be resident on the gateway node itself, in some other device, or its functions may be distributed over several devices. The proxy 708 uses a secure tunneling protocol to authenticate itself to the routers and to control their behavior, but is not so limited. For example, the proxy 708 might instantiate firewall rules on the IP router 702.

5 The router 702 may not know the address of the proxy 708 until it establishes a secure coupling to the proxy 708 on bootup. Devices that need the proxy address, but do not initially receive it, will need to try again after a timeout. The major 10 benefit of using a proxy 708 is that it simplifies the router 702 by handling most configuration. However, for certain operations that demand low latency, the proxy 708 may upload additional data into a DHCP store on the router.

15 Some networks may not support IP because of resource constraints and legacy or proprietary hardware. These networks link into a non-IP router 710. The non-IP router 710 extracts the raw data from packets into an intermediate format and multiplexes them into a single data stream. This data stream is securely tunneled to the proxy 708 (i.e., encapsulated within a secure IP packet). Return traffic from the proxy 708 is demultiplexed and exported onto the appropriate busses using their native link layer protocols. This device has a known address on one of the networks 20 serviced by the IP router 702. The stub protocols in the proxy 708 take on the task of making these non-IP capable devices appear to be IP devices to the rest of the network, so that this larger network can employ IP-based protocols and routers. In this way, security features and the like are added for the longer-range transport of 25 messages from legacy devices or subnetworks, without imposing impractical burdens on these networks or devices.

The proxy 708 acts as a central point for managing security and acts as a proxy for all traffic to and from the Internet. It supports a preloaded set of protocols, but additional protocols can be uploaded. It also manages vehicle internetwork connectivity, and controls what devices are allowed to access the public Internet.

30 The proxy 708 can be implemented on any sufficiently powerful CPU and can reside

anywhere on the network. It establishes secure control channels via encrypted tunnels to the IP router 702 and to the non-IP router 710. It provides stub interfaces 718 (possibly through virtual IP addresses) for services accessible via the non-IP router 710 and associated busses. The routers 702 and 710 and the proxy 708 of an 5 embodiment share authentication tokens to ensure that the correct proxy is talking to the vehicle on boot-up, because many of the security functions of the network are controlled by the proxy 708 , and the embodiment is not so limited.

The WINS vehicle internetwork provides a system in which non-secure messages only propagate within the legacy networks. All messages passed to and 10 from the non-IP router 710 and the proxy 708 use secure IP connections and, thus, the scope for eavesdropping is sharply limited. Further, all other communications within the network can be supported with secure IP, thereby providing the advantages of leveraging broadly available software, and a reduction of protocol translations when interfacing with the broader Internet. Finally, it enables 15 distribution of gateway functions, so that the IP router 702, proxy 708, and non-IP router 710 do not need to be resident in the same physical device.

The proxy of an embodiment can be distributed. For example, the provision of IP and application level interfaces to services on non-IP networks can be located at the non-IP router. This avoids loading network couplings with proxy-specific 20 traffic. Other functions such as acting as the border gateway to a wide area network (WAN) can be centralized at the gateway or distributed as required.

Centralization has a number of advantages including, but not limited to: providing one place to perform security; hiding the decision about which WAN to use behind a single logical gateway; and routing decisions never change as a result 25 of changes in WAN connectivity. Further, if the traffic between the non-IP router and the proxy is tunneled over its own wire, network burdens can be eliminated for this function. Most conveniently, if the gateway itself includes the non-IP router as one of its ports, centralization of functions is easily accomplished. In other embodiments, all proxy functions may be centralized in one location in the initial 30 installation of a system, but as further elements are added to the network, some of

the functions can migrate to other hosts, e.g., additional non-IP routers, or supplemental processors. This results in a lower cost when upgrading the vehicle internetwork.

Other security and translation functions are accomplished through the port nodes, or the network connectors, of an embodiment. A vehicle internetwork can include a variety of port nodes, including non-IP routers, SNICs and PNPs. The port nodes of an embodiment include, but are not limited to, a Serial Network Interface Connector (SNIC) and a Public Network Port (PNP). Both the SNIC and the PNP interact with the proxy to enable IP to be employed over a large variety of buses.

Figure 8 is a Serial Network Interface Connector (SNIC) 800 and an associated internal proxy structure 802 of an embodiment. As an example of device interaction, a cell phone or serial device 804 is coupled via a SNIC 800. The cell phone implements some serial protocol, which the SNIC 800 does not interpret. The serial data is sent back to the proxy 802 which implements a protocol stack to operate the serial link to the phone as well as higher level link protocols such as PPP. Once an IP-capable coupling is established, a new interface is created at the proxy 802 that has an external Internet IP address. Depending on the configuration of the proxy 802, traffic is sent to this address using application level proxies or a network address translator (NAT). Several couplings can be established simultaneously or on-demand, and the optimal coupling can be selected based on factors that include cost per bit and data rate.

The tunnel from the SNIC 800 to the proxy 802 is secure in an embodiment. This security uses reliable transport and cryptographic checksums to accomplish authentication and a guarantee of integrity. For example, this protects against devices that capture and replace packets, for example, to obtain free phone access. In the case of data that is being routed to the Internet, no further security is required. However, certain portions of the serial protocols may need a higher degree of security; for example, traffic from authentication protocols, either to the phone or to the ISP, may include cleartext passwords and other vulnerable data which should be encrypted. The SNIC stream protocol of an embodiment therefore includes an

09580908-42004000

escaping mechanism that enables control messages between the proxy and the SNIC to be inserted into the data stream. One of these commands turns on encryption while another command turns off encryption. The encryption is performed on the data stream and does not affect the escaping mechanism. Another command can be 5 used to inform the proxy when the phone is removed or replaced in the connector cradle. The SNIC devices can establish a coupling to the proxy on bootup, whether or not a phone is in the cradle.

The proxy 802 of an embodiment can implement arbitrary security policies governing external connections. For example, there can be stored authentication 10 data for a driver's telephone, but such data might not exist for passenger telephones. Security and resource management policies can govern the conditions under which an external Internet coupling is established. This architecture reduces the cost and size of the SNICs, since they are not required to interpret all commands of the devices to which they couple. The proxy 802 takes on the higher-level functions 15 that are difficult to implement or of a transient nature compared to the lifetime of the vehicle. The proxy 802 also can accept software upgrades or even convenient hardware upgrades, as it can reside anywhere on the network. Further, reliable streams are established from the boundaries of the network to the proxy 802, with the SNIC 800 capable of being controlled to shut off communications from 20 misbehaving or unauthorized devices.

Figure 9 is a Public Network Port (PNP) 900 and an associated internal proxy structure 902 of an embodiment. The PNPs 900 of an embodiment are distinguished from the SNICs in that the device or network they couple to is IP-capable. Consequently, different functions are provided.

25 The Public Network Port (PNP) 900 is a port node to which any wireless or wireline device may safely couple. It exports a DHCP service which either assigns local IP addresses from a block of local addresses or proxies the DHCP request onto its network. New devices couple to the port 900 and use DHCP to acquire a local address and the address of the "proxy" 902. Initially, the firewall is configured to 30 block all traffic from a new address that is not directed to the PNP port of the proxy

09660608-100400

address. Disconnection of a device from the port 900 is monitored, so that the proxy 902 can be informed and all security permissions for that address may be revoked.

A device may negotiate with the service at the PNP port 900 to extend its privileges. Privileges are associated with specific local IP addresses. This 5 negotiation can make use of an arbitrarily complex security policy. Authentication can be done using any technique available to both the client and the server (software upgradeable on the server). For example, non-authenticated users might be permitted a certain amount of bandwidth on an external Internet coupling, but might not be permitted to cause an on-demand link to be established. Only certain 10 addresses might be permitted to establish such a coupling.

The PNP 900 of an embodiment accommodates different combinations of firewall complexity and the associated efficiency. A firewall with a lower level of complexity lets the proxy 902 make all the decisions and, thus, allows couplings to safe ports on the proxy 902. More complex firewalls allow mobile devices to 15 communicate directly with certain services on the internal network. Design trades are also accommodated with the client-side software. Not all clients will have the appropriate software to perform authentication. On the server side this is managed by implementing various popular authentication protocols. Further, another approach expands the default privileges to include the most typical and innocuous 20 applications, such as low-bandwidth web traffic to public internal services and free external Internet services. This is implemented by changing the default rule set in the firewall, but is not so limited.

External network connectivity can also be available from a wireless gateway that connects via a PNP 900. After negotiation at the PNP server, an IP tunnel is 25 established to the proxy 902 that can be used as an external Internet coupling. The PNP server can also link internal networks that are IP capable. In this case, the proxy ARP causes the multiple devices to appear as one link layer address for the rest of the bus coupled on the other side of the PNP 900. Devices on the internal network can in turn be addressed using a number of techniques. The security

methods used for devices connected to the bus, however, also extend to the devices that are coupled to the internal network.

In common with the proxy/SNIC interaction, the PNP/proxy combination enables device authentication, restrictions to bus access, and secure IP 5 communications over the bus. While the PNP 900 need not host all services required by the IP device, it may pass on much of the burden to the proxy so as to provide a cost and size reduction.

Supplemental Physical Security Measures

10 The proxy/port architecture of an embodiment flexibly supports a variety of supplemental physical means for ensuring network security. For example, the WINS vehicle internetwork supports the fact that the vehicle already includes a security system, namely, an ignition key. Sensors within the network detect if the electrical system of the car is enabled by determining a position of the ignition key, 15 for example, either turning the key all the way or to a position that activates the electrical system. The system accepts the addition of devices to the vehicle network when this activity is detected.

Furthermore, the network can comprise a device that accepts the input of a short password (e.g., a PIN having a prespecified number of digits) for a higher level 20 of security. This device can be wired into the network or be a wireless pad to which security authorization for this operation has previously been given. At this point, the ports on the network will now accept devices being attached, with the identification number of the device being read and added to the library of authorized devices. Further, this security includes devices seeking to couple via the wireless ports. With 25 this method, the devices being connected to the network do not require any built-in security features as the security burden is assumed by the proxy and ports.

Higher levels of security are also supported by the wireless ports of an embodiment. For example, it is possible that someone standing near the host vehicle when the ignition key is inserted and the PIN entered may have a device with AMI- 30 C bus connection capability. This device could be a wireless device that is not

intended to be authorized for attachment to the network. In this case, a security display alerts the vehicle operator in a sequential fashion of all the devices that are not presently registered in the vehicle security database that are attempting to attach. If the description does not match the device the operator was attempting to attach, the operator can decline the connection.

Physical security is also provided in an embodiment using a designated authorization port. The designated authorization port is a port to which connectors are first coupled in order to be authorized for coupling a device to the network. The port is activated by some combination of ignition key detection or PIN entry, but is not so limited. Codes are exchanged which subsequently allow the connector to be used in any matching socket in the vehicle within some specified time window. The connector accepts only one device being attached to it, at the option of the operator, or any device that physically attaches to it. In the latter case, the operator can retain the option of explicitly authorizing the device via a security panel. This method is particularly convenient for enabling installation of consumer electronics, so that the vehicle owner need not be with the vehicle at the time of installation.

In providing security, authenticated devices operating in an embodiment provide an additional level of security to the network and attached devices by including a policy in their protocol that prevents them from forwarding messages to non-authenticated devices. This prevents an authenticated device from receiving messages from non-authenticated devices and passing these messages on through the network. Further, this avoids denial of service attacks, thereby releasing the port or proxy from having to screen the content of all messages.

25 The gateway along with the associated proxy functions provides further security in that it provides a firewall between the AMI-C bus or other consumer networks and the OEM bus. With this firewall, even if an unauthorized device is attached it cannot disrupt the essential functions of the vehicle. The gateway manages the library of authorized devices and the distribution of public keys used in secure communications. Further convenience and security can be obtained if only 30 manufacturer-approved devices can be added to the OEM bus. This need not require

explicit authorization by the vehicle operator if the device to be attached includes the appropriate identification code for the vehicle. The gateway can maintain a library of approved device identifiers for addition to the bus, which is periodically updated through a secure communications session with the manufacturer's service network.

5

Security Scenarios

The proxy/port architecture of an embodiment resists common vehicular security attacks in many ways. For example, consider an attempt to spy on the bus traffic to replay the door lock command, or in general unauthorized issue of a door lock command. Because secure IP communications take place everywhere within the network, an eavesdropper would need to physically attach to the OBD bus, which is connected to the non-IP router. Thus, the eavesdropper would already had to have acquired physical access to a bus that is usually embedded within the body of the vehicle. This is considerably more difficult than simply breaking into the vehicle. Note that since the proxy exports the web interface, it can also broker the door lock button input according to a security policy it maintains. Thus, external attempts are frustrated by policies similar to those used to secure web sites. Privacy is thus enhanced.

In another example of resisting common vehicular security attacks, a Bluetooth device launches a denial of service attack to the servers that control vehicle appliances, or attempts to broadcast video onto the Internet. In the first instance, excessive traffic from the device is detected, and the port is commanded to block further traffic. In the second instance, devices entering the network from an insecure port are explicitly given access to the Internet, for example by means of a pop-up display for the operator or voice authorization.

In yet another example of resisting common vehicular security attacks, consider a PDA being used for a remote banking transaction. In this case, reliance is placed upon the general design that applications assume insecure connections. Thus, the application-level security of the banking application is employed, with the vehicle enabling Internet access by acting as an HTTP proxy.

Secure software upgrades are also enabled in the WINS vehicle internetwork of an embodiment. For example, if the vehicle owner wishes to upgrade the software in the proxy, the proxy presently installed controls the addition of patches to security-critical services, and refuses patches that are not digitally signed by the manufacturer. If third party software is to be added (e.g., to proxy new protocols), then the owner authenticates the installation either in the same way that new devices are attached (if within the vehicle) or by means of passwords and other security procedures (if being effected remotely).

10 **GATEWAY**

Figure 10 is a WINS vehicle internetwork gateway 1000 of an embodiment. The gateway 1000 provides a bridge between heterogeneous networks. For example, the gateway 1000 mediates between but is not limited to four different networks: the OEM bus, the AMI-C bus, an external network (Global network access via a radio port), and a local development network. The local development network includes simple networks comprising a single personal computer and more elaborate computer networks. The local development network can be used to allow developers access to the gateway to permit local upgrade, diagnostics and programming. The bridge function includes both enabling messages to be passed from one network to another, and blocking messages where access is unauthorized. Thus, the gateway can provide a security firewall between two networks.

The local development network, or development port, can be configured to support the manipulation and transfer of entertainment software. The entertainment software comprises entertainment features including video, audio, movies, television shows, music, games, and simulations. The local development network coupling of an embodiment supports the high-speed wireless transfer of information among the vehicle internetwork and remote information stations, but is not so limited. Furthermore, the uploading of entertainment software is supported through peripheral devices and their couplings with the vehicle internetwork.

Further, the gateway 1000 may actually control access to one or several of the networks that it bridges, playing the role of the network master in master/slave networks. In this role the gateway 1000 can instruct misbehaving network elements to shut down, or allow access to particular functions (including being allowed to 5 communicate at all) only according to particular security protocols. Finally, the gateway 1000 of an embodiment serves as the host for the proxy. Thus, the gateway hosts applications that require coordination of several devices on one or more of the networks coupled to the gateway, for example, interactive multimedia sessions or vehicle control functions involving several networks. In exercising this function the 10 gateway 1000 can process the information packets to eliminate redundancy (similar to a data aggregation function) or to prevent inappropriate commands from being passed. As an example, in mediating access between sensors that produce data at some constant rate and a thin and expensive external bit pipe such as a cell-phone, the gateway 1000 can process the data so that only summary reports are passed on.

15 The gateway 1000 comprises, but is not limited to, the following components: a Real-Time Interface Processor (RTIP) 1002, at least one interface port 1006-1010, and an application processor 1004. The application processor 1004 can host parts or all of the proxy. The RTIP 1002 together with the interface components 1006-1010 represents a specialized preprocessor that omits 20 sensing/actuation control functions, while the application processor 1004 handles higher level processing functions. The interface ports 1006-1010 include the physical and MAC layers for the network they interface to, for example the OEM 1006 and AMI-C 1008 buses, respectively, and a radio 1010 and the corresponding protocol, as well as a wired connection. The interface ports 1006-1010 also include 25 buffers so that the various networks being bridged do not have to operate synchronously with respect to one another.

The interface ports 1006-1010 perform a protocol translation function, presenting the RTIP 1002 with data in a standard format for internal processing within the gateway 1000, for example so that it might function as an IP router. In 30 this way, only binary protocol translations are used. This vastly reduces the

complexity when N different ports are supported; only $2N$ translations are needed (N external to internal, N internal to external) versus N^2-N possible translations.

Moreover, internal operations are cleanly separated from any changes that may take place in the protocols for the various networks to be connected to a gateway 1000, enabling greater software and hardware stability.

5 The RTIP 1002 performs the processing to route packets to the appropriate destinations, and issues commands for control of networks for which the gateway 1000 is in the role of master. Thus, the RTIP 1002 performs both the functions of a switch and network master. The RTIP 1002 further routes communications to non-
10 real time systems, such as the application processor 1004. The application processor 1004 can host applications associated with either the AMI-C or OEM buses, such as dealing with passenger conveniences or vehicle operations. These applications are upgradeable via input from the gateway port 1010, the global networks 1020 (e.g. via a web interface on the Internet), and a local development network 1030.

15 While the gateway of an embodiment includes the proxy, hosted on the application processor, and a non-IP router (the interface to the OEM network), many other configurations are possible. A network can include one or more gateways, and gateways can include a variable number of interface ports. These ports can be designed as modular components so that they may be re-used within other gateways
20 and also within port nodes, leading to a lower-cost system. Thus, for example, a gateway can include some combination of ports for the IDB-C, MOST, Institute of Electrical and Electronics Engineers (IEEE) 1394, OBD-II, Standard Corporate Protocol (SCP), Audio Control Protocol (ACP), Bluetooth, Personal Communications Service (PCS)/Global System for Mobile Communications (GSM),
25 Ethernet, and many other wired and wireless communication standards. Further, a gateway can include an interface port to another gateway, so that a larger number of couplings can be supported without overwhelming the RTIP.

POR T NODES

The WINS vehicle internetwork of an embodiment uses an interface for each device that is to attach to buses or other networks within a vehicle. For example, an interface is used between an AMI-C bus, such as the Intelligent Data Bus (IDB-C) or 5 IEEE 1394, and consumer appliances that are supported by the bus. The port nodes perform this function. As part of the interface, the port node performs functions including, but not limited to, physical connection to the buses, physical connection to the consumer devices, protocol translation, and security. Although a port node is used for interface to AMI-C buses, the concept of an interface device has broader 10 implications for vehicle internetwork embodiments, namely, the non-IP router, SNIC and PNP devices.

The WINS vehicle internetwork supports interfaces with consumer electronics without a requirement for manufacturers of the consumer electronics to embed special connectors in the consumer electronic devices or to specially 15 configure the devices for the vehicle network interface. In this way, legacy devices or devices designed for a broader consumer market can be added to the network so long as a port node which includes the necessary physical mating and protocol translation is available. Examples of devices that might be added include but are not limited to audio equipment including compact disk players and speakers, DVD 20 players, video cassette recorders (VCRs), computers, and computer peripherals. Consumers are now used to buying special connectors for vehicle electrical outlets; port node adapters are the network connection analog.

As another example, a port node wireless adapter can include a radio that communicates to another port node coupled to the wired network. Thus, devices can 25 be added without requiring physical connection. This both reduces the number of ports that are provided in any vehicle retrofit, and enables devices such as PDAs, cellular telephones, and computers to be conveniently added or removed from the network. Further, wireless port nodes can be designed with particular protocols (e.g., Bluetooth) that can directly network to consumer products. By this means, no 30 modifications are required of the consumer products.

Similarly, port node adapters can interface a wired subnetwork to the AMI-C or OEM bus, for example the audio system. Also, protocol translation can be provided for any mixed wired or wireless network. Components and software for such adapters can be shared with interface ports for the gateway to reduce 5 development effort.

Figure 11 is a port node architecture 1100 of an embodiment. The port node 1100 includes protocols for two different networks, with at least one of the appropriate line drivers, or radio modems, for each side. As an example, in bridging between an AMI-C bus, specified as IDB-C, and a Bluetooth radio network, the port 10 node includes a bus interface 1102 that includes on the AMI-C bus side both the IDB-C protocol and associated line driver as well as a proprietary high speed driver that operates during assigned slots to communicate with like devices attached to the bus. Coupling the bus 1102 and appliance 1104 interfaces is a micro real-time 15 interface processor (μ RTIP) 1106. This device performs a subset of the functions that might be performed by the RTIP in the gateway, in that it is dealing with only one connection and is not controlling the networks on either side. Its functions include instructing the interfaces on the proper rates at which data can be transported, including the capability to block inappropriate transmissions across the 20 device.

The port node 1100 further includes a memory cache 1108 for storage of policies that it may download from the gateway or other devices for support of services including security/authentication and prioritization of resource requests. The cache 1108 also has storage available for short-term queuing of information, for example, for the interval between slot availability on the two sides of the interface to 25 allow the networks to operate asynchronously with respect to one another.

Figure 12 is a safety connector 1200 of an embodiment. The safety connector 1200 is provided in furtherance of passenger safety and the avoidance of consequences associated with malfunctioning devices flooding the bus 1299 with spurious data. As such, this safety connector 1200 avoids having to directly attach 30 network devices to the terminals of a bus 1299. Thus, while port nodes can be used

that directly attach to the bus 1299, for the passenger side of a network these can be supplemented by a simple connector that shields the bus 1299 and vehicle passengers from danger.

The safety connector 1200 includes circuitry 1202 for detecting a physical fault such as a short on the exterior side of the safety connector 1200, but is not so limited. This circuitry 1202 activates the control circuit 1204 to command physical isolation 1206 across the connector, e.g., by opening a switch. The protocol violation detector 1208 interprets commands from the gateway to isolate the two sides when necessary, as in response to a device that is flooding the network with access requests, or which is sending unauthorized messages. Additionally, the protocol violation detector 1208 includes circuitry to recognize that insistent use of the bus is being demanded by the device that is attached, so that it can command physical isolation.

15 **MODULAR VEHICLE INTERNETWORK**

The vehicle internetwork of an embodiment includes highly modularized components, wherein a distributed architecture is provided that allows for customization of components in support of diverse applications. The modularized components provide for reduced cost of individual system components, independent component engineering, and an API set that is independent of the hardware on which it resides.

Functions of the WINS NG system in an embodiment can be partitioned so that components are reusable among different product families. When partitioning components, the RTIP functions as a high-speed bus passing IP packets, with control residing at the devices with which it interfaces or couples. The gateway takes on the functions of an IP router, with additional functions related to security. Depending on the processors and ports to which the gateway is coupled, it serves as the core across a number of applications including, but not limited to, the sensor,

diagnostic/prognostic, telematic, and AMI-C applications. Ports, depending on the interfaces used, can become tags, bridges, or network interfaces.

Regarding node architecture, Figure 13 shows a number of ways a WINS
NG system of an embodiment can be reconfigured to accommodate different
5 applications. For telematic applications, the processor 1302 may be identified with a
telematics processor. For diagnostic/prognostic applications, the processor 1302 can
be configured as it would in sensor node applications. The legacy OEM port set
1304 aggregates information for more efficient use of the RTIP 1306, and avoids
10 using a large number of its interfaces. For AMI-C applications, there can be
additional processors 1310 and 1312 coupled directly to the RTIP 1306 or coupled
through the high speed network, or a combination of both as a result of upgrades
over the life of the vehicle. For sensor applications, the automotive ports are
15 replaced by sensor ports.

The WINS NG ports of an embodiment contain an interface that results in IP packets being passed through the RTIP, but are not so limited. As a result of scaling, shared resources such as memory and processing are not embedded within the RTIP itself; it is much more difficult to construct software that can deal with additional ports when there is frequent contention for a scarce common resource. However, to accommodate occasional demands for more memory, an embodiment includes extra memory and processing available through a particular port or ports, thus reducing the overall memory requirements compared to placing all such resources in the individual ports.

Likewise, security firewall operations are not directly performed by the RTIP of this embodiment. Instead, packets addressed to the OEM side are examined by a processor, and then forwarded, wherein the processor resides within the OEM port, or elsewhere. For example, a security processor can issue tokens which then allow such devices to directly communicate to some other location. While not precluding the first RTIP from being a processor that integrates switch and port functions, however, the use of standard interfaces provides modularity.

The modular switch architecture of an embodiment includes a hybrid architecture that enables the switching fabric to be built up from a set of stand-alone modules, thereby enabling varying tradeoffs between total memory requirements and the speeds of the components. While some embodiments include relatively low-speed ports, some embodiments are capable of supporting high speed ports such as the IEEE 1394.

5 **Figure 14** depicts a hybrid switch architecture 1400 of an embodiment. The architecture 1400 includes at least one interface port 1402 coupled among at least one high speed switch 1410 and at least one low speed switch 1420 or lower speed switch. The high speed switch 1410 and the lower speed switch 1420 are each 10 coupled to at least one port 1404.

15 As an example, the lower speed switch 1420 can be used in diagnostic/prognostic and telematic embodiments, while the medium/higher speed switches 1410 or modules are used with AMI-C products. This approach has the advantage of matching switch specifications to the demands of highly varied input ports. Thus, not every component must operate at the highest speed, and the appropriate switch architecture can be separately considered as higher performance ports are added to the system.

20 The modularity of the units also enables, for example, the coupling of multiple low speed switches to a medium speed switch. If internal packet formats and addressing conventions are the same, the interface port among the switches becomes very simple. Thus, in common with other WINS NG technology applications, processing and communications are matched to the resources demanded by an application.

25 The distributed switch architecture 1400 further supports distribution of the switching functions throughout the vehicle. Consequently, all of the buses and ports of the WINS vehicle system are part of the switching fabric. Therefore, an output buffer switch in effect distributes switching along the length of the corresponding bus. As a result, independent development and improvement of WINS vehicle 30 switch components is supported throughout the life of the system.

A number of basic packet switch architectures can be used within the modular architecture of an embodiment. These typical switch architectures include, but are not limited to, distributed buffer architectures, shared buffer architectures, output buffer switch architectures, and input buffer switch architectures.

5 Limitations of particular architectures lead to the use of either the shared buffer architecture or the output buffer switch architecture, wherein advantage is taken of either a low part count (the shared buffer architecture) or use of standard high-speed buses such as an Ethernet or IEEE 1394 (the output buffer architecture).

10 Using a shared buffer architecture, a common pool of buffers is divided into linked lists indexed by the output port name. There are no crosspoints as such, with all routing based on these indices.

15 The output buffer switch architecture includes a multiplex buffer for each input (to match rates), a time-division bus which acts as the switch, and address filters and output buffers for each output. An advantage is found in the ease of programming in multicast.

20 In the diagnostic/prognostic and telematic applications, an interface is used between legacy OEM networks or ports and the processor. The shared buffer architecture is used in the interface, as transfers are relatively low speed. For each port, some number of inputs are buffered and then assembled into a packet; for convenience, all packets are of the same size and have the same addressing convention. They also get transmitted at the same speed. These then get passed through the shared buffer, which handles the queuing.

25 In an alternate embodiment, buffering is performed at the processor port (input buffering for downstream, output buffering for upstream), with the protocol conversion and rate matching taking place at each OEM port. The buffering includes input buffering for downstream transfers and output buffering for upstream transfers. Data is transferred to and from the processor port using either a bus (e.g., one for which there is already an interface written for the processor), or a tree structure.

00004000-4000-4000-4000-40004000

In extending the architecture towards AMI-C, an additional output port can be included that enables the addition of a second switching stage. A buffer between the two stages performs rate conversion between the OEM switch and the higher speed switch. This buffer can be of the output buffer type, for example, eliminating one interface by having the switching bus as the highest rate component. Because there are few high-speed buses in the vehicle, the additional parts count compared to a shared buffer architecture would be slight, given the more substantial multiplexing/rate conversion effort required for high-speed buses.

In an alternate embodiment, a medium speed switch and associated buffers are coupled among the high speed switch and other switches or ports. The medium speed switch can use either the shared buffer or output buffer architecture. This provides great flexibility and supports independent component design as the interface between the stages converts the internal packet format/address convention of the succeeding stage.

Figure 15 is a port architecture 1500 of an embodiment. The communications interface 1502 includes at least one line driver, protocol translation, and packet encapsulation, but is not so limited. When coupled to the RTIP, the communications interface 1502 serves as the interface to the RTIP.

The micro RTIP 1504, or μ RTIP, may simply be a bus, possibly of the same type as in the RTIP but with fewer couplings. If it is the same as an RTIP, the communications interface to the RTIP becomes trivial. Alternatively, the μ RTIP 1504 functions along with many functions of the two interfaces can be performed by the port's real-time processor, for example, within a tag.

When IP networks are coupled to both sides of the port 1500, a small router directs packets from the appliance interface 1506 (for example, from a sensor, actuator, or communications device) to be queued in memory 1508, and possibly be examined by the processor (for example, for security purposes). Alternatively, if used as a tag, the appliance interface 1506 is to a sensor and the communications interface is to a radio. The processor then directs the activities of the tag.

SERVICE DISCOVERY AND APPLICATION PROGRAM INTERFACE

Internet service discovery protocols such as Jini technology demand large memory and computational resources, and provide limited network self-assembly functions. By contrast, the WINS vehicle internetwork enables complete self-assembly of a network and its applications, including coupling to services in outside networks. These methods are used for vehicular applications so that minimal expertise is required of the vehicle operator or installers of new devices, and so that the network components can be low-cost. After self-assembly has occurred using these protocols, Jini or a similar protocol sitting above the IP layer can be invoked in the higher-end devices so that standard software applications can be used. For clarity of discussion of self-assembly and service discovery, the descriptions herein assume that the proxy is hosted on the application processor of the gateway. However, alternative arrangements accommodate hosting of proxy components.

Self-assembly and service discovery occur in two distinct fashions. For devices with direct port node couplings to buses leading to the gateway, the gateway directly mediates the assembly functions, analogous to a network gateway in star topologies. For devices that belong to a subnetwork, a separate protocol is used for subnetwork assembly. The port node that interfaces the subnetwork to the bus then passes service requests to the gateway. In this instance, the port node may for example be either a PNP device or a non-IP router.

When attaching to a network a node acquires synchronism, announces its presence, is authenticated, and publishes the modes by which it can communicate. Service discovery makes the node aware of the resources available in the network. A node joining the network first listens to traffic to synchronize to the control channel of the gateway. It then responds in one of the slots provided for nodes to request service, indicating its identity and capabilities with a unique code. The gateway can then consult its security database to determine whether the device or network of devices attached to the port node is authorized to communicate. If any devices are not authorized, a sequence of operations as described herein is pursued

0960608-400400

00000000000000000000000000000000

to establish authorization or instruct the port node to prevent any traffic from the unauthorized devices from being passed on to the network.

5 The gateway maintains a database for both policies (e.g., security, service configurations) and data, with permanent and transient entries. The policy database enables port nodes to download instructions in support of particular services.

Consequently, not all services need to permanently reside on the port nodes. Port nodes can request participation, or respond to invitations, for particular services by exchanging codes that index the services of interest. One code, for example, could be reserved for establishing a Jini session, setting in motion the process of invoking 10 higher levels of service discovery. Another code might be a query for resources of some particular type, to which the gateway responds with a listing of addresses of nodes. New policies can be added to the database either through the system's external connections (mediated by the gateway) or through the bus.

15 Transactions among nodes on the bus use the gateway in mediating access to the bus, when the gateway assumes the role of a master. However, unless a message is to be passed through the gateway to another network, it will not usually need to decode transmissions from one port node on the bus to another port node. The gateway may or may not mediate access to a multi-cast group performing some particular function, beyond reservation of slots. Involvement by the gateway in such 20 operations is determined by whether the nodes are capable of managing the session themselves. Consequently, the gateway is an active participant in mediation when the nodes are not capable of managing the session.

25 The gateway of an embodiment mediates services that go beyond any single network to which it is coupled, including multiple networks within the vehicle and external networks. The gateway policy database therefore contains protocols for service discovery in diverse networks. External network connections further account for the variable communication rates that are typical of links to vehicles. For example, service islands of high-speed connectivity (e.g., within a garage or at a service station) may exist, providing low-cost and high-speed download capability 30 (e.g., for audio or video entertainment). The gateway may thus command download

when communication conditions are favorable in anticipation of later demand. To this end, the gateway accesses mass storage so that such transient material can be stored until it is used. Note, however, that while the gateway may be executing this service policy, some other device connected to the network can be in charge of the 5 requests, and be the origin of the policy. The gateway in this circumstance is in the role of mediating the competing demands for resources according to the priorities expressed in their service requests.

The service architecture includes a number of levels, any subset of which can interact. Services may be confined to subnetworks attached via a port node, in 10 which no demands are made of the general vehicular network. Services may be confined to one bus attached to the gateway, or may involve both a bus and subnetworks connected to that bus. Alternatively, services may also include connections outside the vehicle. Such a network resembles the Internet in many 15 respects in that heterogeneous networks are tied together with gateways that perform routing and queuing functions. In the WINS vehicle internetwork, however, the port nodes and the gateway take further responsibility for self-configuration and security authentication, with minimal human operator involvement. Moreover, the components are themselves low cost, in contrast to Internet routers and gateways.

Figure 16 is a vehicle internetwork application programming interface (API) 20 structure 1600 of an embodiment. The vehicle API 1600 lists services 1602, host 1604, and API examples 1606. Services 1602 include application support, database services, routing, security, network management, and deployment. The application support, database services, and routing are hosted on the gateway. The security, network management, and deployment functions are shared among the gateway and 25 nodes.

Figure 17 shows a gateway hardware and software interaction 1700 of an embodiment. The gateway RTIP 1702 is performance and cost-optimized for supporting the lower level functions 1704 such as routing, security filtering, and application support for higher level applications. The API 1710 includes an open 30 messaging set 1712 that enables a variety of platforms to sit on top of the RTIP

00000000000000000000000000000000

1702. Such application processors 1710 can then use any of a number of different operating systems and programming languages being at once shielded from the real-time operations of the RTIP 1702, yet able to control the functions being executed and access raw data as required.

5 **Figure 18** shows application programming interface (API) layering 1800 of an embodiment. The lower level 1802 includes functions particular to the vehicle internetwork, including gateway and port node operation, implementation of AMI-C and IDB-C bus protocols, security, routing, network interface support, and low-level services. The software for these functions has a relatively small footprint that
10 enables the devices to be low-cost. At the same time, the APIs permit higher levels 1804 and 1806 to access parameters or data managed at the lower level 1802 so that information on the state of the network can be retrieved, and parameters re-set to control its behavior. The application processor in the gateway or in consumer devices attached to the gateway includes an operating system (OS) 1804 that
15 interfaces with the lower level 1802, and enables higher level applications 1806 developed for more powerful platforms to be used. For example, Java or Jini 1806 may run on top of this OS 1804, so that standard applications developed for broad consumer markets can be executed.

20 **Figures 19 and 20** show an example of how a layered set of APIs work in an embodiment. **Figure 19** shows default device discovery of an embodiment. A low cost consumer device 1902 coupled to a port node becomes integrated into the network with the default discovery service 1904, i.e., the lower layer APIs related to service discovery. The device goes from a state of having no knowledge of the network, to becoming an integral part of it. All the levels up to the link layer are
25 dealt with, as is a set of applications.

Figure 20 shows Java/Jini application enablement in an embodiment. The default discovery process takes place, but in this example it is determined that the device 1902 can support Java and Jini 2002. Thus, using the same lower level protocols, a higher level application discovery can now take place using Jini, leading
30 to support for more sophisticated application sessions involving, for example,

09680608-14004000

several consumer devices, the gateway, and remotely located devices on an external network such as the Internet.

Vehicle internetwork service discovery of an embodiment among non-Java capable devices uses a scalable protocol, wherein the protocol can be used across a 5 broad range of devices using the WINS technology. The service discovery protocol may be configured to support a single node as a focal point or proxy. However, the protocol also supports the notion of a service region, wherein nodes are unwilling to offer or request services from distant nodes or nodes which lack security authorization. The service region can depend on the priority expressed in a service 10 request. Thus, all messages include fields expressing priority and reach of the message, as well as identifiers for the services being registered or requested.

The service discovery protocol includes a set of messages and transactions that enable the support of a broad set of distributed services, as well as services that are coordinated by one central node. The messages and transactions include, but are 15 not limited to, find service locator messages, service advertisement messages, service queries, service query responses, service code translations, and service requests.

The find service locator message is a multicast that includes a range indication. For the vehicle internetwork, this message can do double duty that 20 includes identifying a new node to the network, since all find service locator messages are routed to the proxy. For a WINS NG network, potentially every node has a service registry, and so this message indicates the region over which nodes are to be identified.

The service advertisement message is provided to service locators and 25 includes codes for available services. Message components can also include a status for serving requests including withdrawal of service availability, and classes of nodes that may request service. In the vehicle internetwork, the proxy will determine classes of nodes that are eligible for such services under the security protocol. The codes include, but are not limited to, Bluetooth Service Discovery 30 Protocol (SDP) codes, and other application-specific codes that indicate Java-

capable nodes, or codes related to authentication that implicitly identify services. A code can be reserved for service locators.

The service query is a request to service locators indicating codes for services requested, propagation range of the query, and priority of use. The service query can also request lists of services.

The service query response is a response to a service query from a service locator that includes addresses of nodes that can provide services. The addresses can be formatted as prioritized lists. The address may actually be the proxy address in some cases when the proxy performs code translation. The proxy will deny requests that violate the security protocol.

Service code translation is performed so that applications running on the nodes that are involved in services are able to provide or request a service identified by the code. In some cases, this translation can be performed by the proxy.

Service requests are requests for service from nodes to devices whose address has been provided by the service locator. Service requests indicate service codes and priority levels.

Mobility is an important factor in service discovery and data integrity. Atomic transaction methods are used to deal with intermittent connectivity. While atomic methods are standard, for example, in distributed database problems (e.g., the Commitment, Concurrency and Recovery (CCR) application service element for maintaining integrity in shared access applications), the problem in mobile systems is not always a matter of preventing multiple users from making inconsistent changes to a database. Rather, the issue associated with the WINS vehicle internetwork is to efficiently download and upload data between a mobile and any number of fixed terminals.

For example a vehicle may upload operating system software or entertainment products through short range, low-cost links. However, it may move beyond the range of one such short range transmitter before a transaction is complete. When this happens, such information is logged in the database so that when connectivity is established with another transmitter the record download

begins again where it left off. Alternatively, the mobile unit can record how many packets of a message have been received or transmitted, and instruct the fixed infrastructure at which location in the record to begin retransmission. The database system for mobility management could in this case predistribute code and data to 5 projected Internet gateways along the likely paths in anticipation of the arrival of a specific vehicle, or a vehicle that belongs to a class, all of whose members use the same data. This minimizes down-time of the wireless links while waiting for information over backbone satellite or wired networks.

Conventional atomic transaction methods are appropriate to managing the 10 distributed copies of messages to mobiles, in that they should delete data that has already been successfully transmitted to all members of a class, and forward only data within a session that has not already been transmitted. In this way, the backbone network transmits less data over long hauls, and has lower average storage requirements. With such atomic transaction methods, the requirement for 15 continuous high-speed coverage is eliminated, and flexibility for transmission of records over multiple communication means is provided. Service discovery transactions can proceed in a similar fashion. In effect, the proxy and remote database interact through a variety of means, possibly accessing systems such as the vehicle navigation system to predict the best links to use.

20

BUS PROTOCOL

Embodiments of the WTNS vehicle internetwork enable more efficient usage 25 of the associated buses. In one embodiment, more signal processing takes place at the source (e.g., sensors) so that processed rather than raw data is sent to other components of the network. Also, multiple low speed devices may be coupled on a separate physical wire, with aggregation of their data at an interface device to the IDB-C bus (e.g., a port node), thereby lowering the cost of their communications connectors.

In an alternate embodiment, higher speed communications are enabled in 30 time slots reserved using the IDB-C protocol. Access requests are broadcast and

00690608-1000000

slots assigned. A proprietary protocol can then be used during that slot to achieve a high speed burst of data. This approach has the communication devices for the parties to the conversation understand both the high speed and the IDB-C protocol, but does not require other devices to have anything more than IDB-C. Thus, support 5 for heterogeneous protocols is automatic, and gradual upgrading can take place.

Through the use of subnetworks, devices with very low speed requirements can avoid having to implement the IDB-C protocol. Further, by using the IDB-C protocol simply to schedule transmissions, higher speed devices can be added to the network. It is also possible to use line drivers for other applications (e.g., 10 MB 10 ethernet), with minimal modifications, thus leading to low costs. The result is that devices with a huge range of communications requirements co-exist on the same network.

15 **WINS VEHICLE INTERNETWORK EMBODIMENTS AND APPLICATIONS**

WINS Vehicle Internetwork Embodiments

Figure 21 is a WINS vehicle internetwork 2100 of an embodiment. The vehicle internetwork 2100 includes at least one gateway 2102 coupled among an 20 OEM network 2110 (depicted as a single bus, but not so limited) and an IDB-C bus 2120. Vehicle functions supported on the OEM network 2110 include climate control systems, positioning systems like Global Positioning System (GPS), video/audio systems, cellular systems, embedded PC multimedia systems, vehicle sensor systems accessed via the OEM OBD-II port, and control of lighting, door 25 locks, and other functions via the SCP bus, but are not so limited. Devices supported on the IDB-C bus 2120 include, for example, GPS units, PC-based multimedia devices, and PDAs.

The gateway of an embodiment includes an application processor which hosts the proxy, and consequently supports the network management, service 30 discovery, security, and wireless access. The gateway bridges among the IDB-C,

SCP, OBD, local area wireless, and cellular wireless Internet protocols. The port nodes interface the consumer electronic devices to the IDB-C bus, and thence to the gateway with its many couplings.

The gateway also includes a wireless access port for local area networking.

5 The wireless access port includes a 2.4 GHz frequency-hopped spread spectrum modem channel, functionally equivalent to the Bluetooth wireless standard. This port provides connectivity to a local area wireless Internet access point. This link provides secure, local area Internet and web access to the vehicle system.

Figure 22 is a WINS vehicle internetwork system 2200 of an embodiment.

10 The system 2200 provides self-assembling components that form a wireless network among vehicles 2202 and local sites 2204, which can, for example, be located in a residence, service station, maintenance shop, or parking lot. Connectivity is available for vehicle service, and data transfer to and from the vehicle 2202 (e.g., for maintenance history, email, linkage to the Internet or to provide entertainment

15 services). The internetwork further includes bridging among the vehicular networks 2202 and cellular modems or services 2206, which may for example provide PCS and GSM wide-area access to the Internet 2299. Among the functions enabled are remote access to controls, diagnostic data and security functions via standard Web interfaces, and exchange of email. Other electronic services supported include

20 access to a server 2210 enabling global Internet access. With this access, a SQL server can be used to provide database services for management of vehicle data systems. A web server 2212 can provide secure access for data upload and download between authorized users and vehicles.

Figure 23 is a WINS vehicle internetworking system 2300 of an alternate embodiment. Vehicles 2314, 2316, and 2318 can each be manufactured by a single manufacturer or different manufacturers. The vehicle manufacturer installs the WINS internetwork system components in the vehicles to allow internetworking throughout the life of each vehicle. The manufacturer's existing information technology systems 2306, including WINS vehicle information servers 2320, are used to participate in the WINS internetworking system. Through gateways 2308

00660606-40000

and 2310 and the Internet 2312, world wide web access to WINS vehicle information servers is provided to vehicles 2314, 2316, and 2318. Because communication in the internetworking system is two-way, WINS vehicle information servers may also access individual nodes, such as gateways 2308 and 2310, and individual vehicles. The WINS vehicle information servers can also be placed in any location apart from the manufacturer's existing information technology systems 2306. The WINS vehicle information server 2304 is an example of a vehicle information server that can exist anywhere.

Computers having access to the web, such as computer 2302, have access to nodes, vehicles, and WINS vehicle information servers. Computer 2302 can, for example, be a home, office, vehicle dealer, or service station computer. Communication among vehicles 2314, 2316, 2318 and any of the gateway nodes, such as gateways 2308 and 2310, is accomplished through wireless links that do not require universal high-speed services, but may include a mix of low-speed wide area couplings and high-speed short range couplings. Communication among gateways 2308 and 2310 and the Internet 2312 can, in various embodiments, be accomplished using wireless or wireline methods.

In vehicle maintenance applications, the WINS vehicle internetwork can include WINS NG nodes. These nodes provide low cost, low power, compact intelligent nodes that can be coupled to vehicle diagnostic ports. Such nodes can communicate using a number of communication modes, including the FCC industrial, scientific, and medical (ISM) band spread spectrum channels. These channels, in addition to providing robust communication, are unlicensed, thus eliminating wireless access subscription fees for short range coverage. Power limitations, however, may affect wide area coverage, so communication over such channels may be supplemented by lower speed access over licensed channels (e.g., via cellular modems), with access mediated by the proxy. The WINS NG nodes link to local area WINS NG bi-directional gateways that access Internet services via multiple channels. The WINS NG node manages the vehicle access port, logs

00660608-100000

vehicle information, finds WINS NG network Internet access, and immediately enables a wide range of valuable services at small incremental cost.

WINS Vehicle Internetwork Applications

5 The WINS vehicle internetwork can be used in a wide variety of applications, including vehicle assembly, vehicle maintenance, fleet management, fleet reliability analysis, anti-theft systems, support for entertainment systems, coordination of vehicle systems with consumer electronics, and targeted advertising. The WINS vehicle internetwork includes functionality that provides numerous 10 advantages while enabling this broad range of vehicle reliability and consumer services. The functionality includes, but is not limited to: self-assembly and authentication from physical layer through to applications; providing the ability to control physical parameters using APIs while using high-level and standard software tools; separating real time and non-real time processing; flexible proxy/port 15 architecture; integrated database management; flexible processor architecture; Internet access and control of network resources; and use of web tools and remote databases. Thus, individual vehicle systems can be monitored, queried, and upgraded on a global scale. Internet services provide remote access that can be integrated into the operations of a vehicle manufacturer. Vehicle internetworking 20 provides benefits through the entire vehicle life cycle from manufacturing, distribution, sale, fleet or individual owner information, maintenance, regulatory compliance, and used vehicle sales information.

25 In the area of vehicle reliability services, the same basic infrastructure can be used throughout the life cycle of a vehicle, from factory assembly through operation of the vehicle to ensure its reliable operation. During vehicle assembly, for example, WINS NG networks can provide low-cost monitoring of the reliability of an assembly process. The WINS NG network self-assembly features enable convenient retrofit of factories, condition-based maintenance for assembly machinery, and attachment of nodes to parts for tracking and inventory purposes. 30 Further, WINS NG networks include interaction with standard databases, and thus

the assembly history of the vehicle can be stored using convenient software. When the WINS vehicle internetworking system is installed in the vehicle, the OBD port can be remotely queried and the test operation of the vehicle added to this database, providing the capability of relating any flaws to assembly conditions. In conjunction 5 with data collected over the lifetime of the vehicle, such a database of conditions of the vehicle from assembly through break-down can be used to improve assembly methods.

Further in the area of vehicle reliability services, data access to vehicles can encompass many measurement capabilities that are of use to both the vehicle owner 10 and the manufacturer in maintenance support over its lifetime. The On-Board Diagnostics standards, OBD-I and OBD-II, provide access to a wide range of parameters useful in assessing the status of vehicle systems. In one embodiment, an application hosted on the gateway application processor collects histograms of the different parameters, and stores records that deviate from standards predicted by the 15 manufacturer. These records and the performance histories are downloaded to a database maintained by the manufacturer, or some third party, via low-cost Internet couplings. These Internet couplings may be, for example, over a short range radio link when the vehicle is parked at the residence of the owner. Diagnostic and prognostics software can then be run, and if a problem is suspected, the vehicle 20 owner is alerted to the need for maintenance. Further, this software can command changes in what data is collected, as more information is required in tracking down particular problems.

In a complimentary application, if on-board vehicle diagnostics indicate an emergency situation, the vehicle operator is immediately alerted and provided with 25 information on the nearest repair locations. The alerting, as a result of its higher priority, may use higher-cost wider coverage communications such as two-way paging or cellular telephones.

In yet another application, driving habits of the owner can be analyzed over time and correlated to the apparent wear of vehicle systems. This information can 30 be used by the manufacturer in designing new models to conform to the manner that

the vehicles are actually used, or to alert drivers to habits that may result in costly repairs if continued. Moreover, the ability of vehicle internetwork servers to issue queries that also affect how data is collected can lead to deeper investigations of priority events, without requiring this level of detail over all time or across whole fleets.

5 The WINS vehicle internetwork also enables convenient software upgrading, through the many communications means available, and the management for low-cost access performed by the proxy. Further, the self-authentication and self-assembly features enable incorporation of new devices into the network that upgrade 10 the hardware capabilities, and thus support for more sophisticated applications (e.g., enhanced vehicle prognostics and diagnostics). For example, additional diagnostic devices such as WINS NG nodes can be conveniently added. These additional diagnostic devices supplement the information provided through the OBD port at the time of manufacture.

15 The WINS vehicle internetwork further enables auditing of repairs performed on the vehicle. Since a database of vehicle performance is assembled prior to the repair, an expanded diagnostics capability is enabled, potentially available to each of the owner, repair shop, and manufacturer via the Internet and using standard web browsing tools. This reduces the errors made in diagnosing the 20 problem, since the repair shop will now have access to how the vehicle is performing in a variety of conditions, rather than only its static performance in the repair shop premises.

25 The performance of the vehicle after the repair can be compared to its history prior to the repair to determine whether it was effective. Thus, repair shops and the manufacturer can both audit their procedures, potentially over entire vehicle fleets, to determine which procedures are the most effective for particular problems. This will ultimately lower the cost of repairs, reduce fraudulent repair practices, and enable comparisons to be made among different repair shops. Further, such maintenance records can be made available at time of sale or re-sale of a used

vehicle. Thus, more complete information can be obtained, enabling more realistic pricing and more equitable resolution of disputes regarding pre-existing conditions.

The collection of actual vehicle performance data is extremely valuable for the manufacturer as the above examples illustrate; for the first time assembly 5 conditions, driving habits, and maintenance operations can be correlated to vehicle performance. The WINS vehicle internetworking system enables economical operation of these functions through the data and communications management performed by the proxy, and the use of WINS web servers with their couplings to standard databases. Information about particular vehicles is also valuable to the 10 owner, but aggregated information over fleets can greatly assist a manufacturer in providing upgrades, deciding upon recalls, or designing future generations of vehicles. Additionally, it can assist in regulatory compliance.

Such information about actual use can also be very valuable to owners of fleets, such as rental car or trucking companies. This can assist in pricing of 15 services, scheduling of maintenance, and determining which makes of vehicle provide the most robust performance. Such agencies can maintain high-speed Internet couplings at rental locations or depots, so that even without wide-area deployment of high-speed services they can obtain frequent updates on vehicle status. Inventory management is also assisted since vehicle locations can be 20 implicitly determined by tracing the routes of communications sessions, or explicitly determined if the vehicle includes a navigation system. Further, customer satisfaction can be enhanced through automated help desks that are reachable by the wide area communications means of an embodiment. In this manner, personalized services can follow individuals as they move among different vehicles.

In the area of consumer services, the WINS vehicle internetwork of an 25 embodiment provides a number of applications including, but not limited to, coordination of vehicle systems, vehicle entertainment uploads, targeted advertising, privacy profiles, and owner/operator profiles. The gateway of an embodiment can coordinate a wide range of vehicle systems from actuators to communications ports.

30 Since the APIs provide high-level software access down to the physical layer,

standard methods can be used to provide unprecedented interaction among vehicle and consumer systems, thereby enabling a wide variety of applications.

In the event of the theft of the vehicle or other unauthorized vehicle operation, the owner can report its loss and initiate any of a sequence of procedures 5 to enable its recovery via the WINS vehicle internetwork. For example, the proxy can be paged to interface with the vehicle navigation system to continuously report location to law enforcement agencies. In a complementary measure, when the vehicle comes to a halt, the computer controlling the engine can be commanded to shut down so that the vehicle cannot be operated. In a refinement, the vehicle 10 slowly comes to a halt when law enforcement enters its vicinity. In yet another measure, alarms, loud speakers, and other devices can be commanded to operate to render unobtrusive vehicle operation impractical. Such scenarios further underscore the need for the security protections provided by the WINS vehicle internetwork, since unauthorized command of these activities can be extremely damaging.

15 In another example of coordination of diverse systems of an embodiment, when an incoming voice-call is detected, the volume controls on the stereo system can be automatically damped, and windows closed to reduce the background noise. In this example, systems on the consumer side of the gateway would operate in tandem with controls on the OEM bus. The diverse communications supported also 20 enable other coordinated actions, for example remote vehicle activation to load narrated web news, and to start the air-conditioning (or defrosting) prior to it being entered by the owner. Such actions could for example be coordinated according to a profile of operator preferences, which can be explicitly commanded, or adaptively created through observation of actual operations.

25 The mobile IP management functions of the WINS vehicle internetworking system enable economical uploading of video or audio entertainment. The volume of data required for such applications is large, and consequently providing continuous wireless access over large areas can be very costly. However, upload costs can be essentially free at short range, for example, if the residence is equipped 30 with a short-range high-speed wireless link. In another embodiment, audio

00000000-400400

entertainment can be uploaded at filling stations or other locations in which the vehicle is likely to be within a short distance of a high-speed transmitter.

Once in a vehicle, consumers are more likely to consider making purchases. Of particular interest are retail outlets within a short driving range. A variety of 5 means exist to multicast this information to vehicles, including short range radio broadcast and interactive web sessions based on user preferences. Communication devices and applications for interaction with the WINS vehicle internetwork may be paid for by the advertising service, or Internet access provided for free on condition of subscription to such services.

10 The WINS vehicle internetwork security functions also enable privacy operations. Particularly sensitive matters include vehicle location and speed, and conversations within the vehicle that may be accessed by the hands-free microphones of a cellular system. The owner must have control over which parameters are uploaded, and in what level of detail (aggregation). At different 15 times and places and for different purposes (e.g., law enforcement, manufacturer, vehicle service) the preferences may change. The WINS vehicle internetwork of an embodiment manages this by supporting privacy profiles, resident both on the vehicle and some remote site, which the owner accesses via passwords. Operators can similarly possess profiles that pass, for example, to rental vehicles, but which do 20 not supersede the owner's profile (of course, the owner's profile may permit temporary replacement by an authorized operator).

The vehicle internetwork of an embodiment can incorporate many vehicle operator/owner preferences beyond privacy concerns into owner profiles. The owner profile can have priority over other profiles, with the ability to allow 25 authorized operators (e.g., someone who has rented the vehicle) to upload their preferences. In this way, preferences for privacy, seat and control position, appropriate actions during cell phone calls, and quality of service for external network couplings can follow operators between different vehicles. Such information can be embedded in smart cards, but is not so limited.

The description herein of various embodiments of the invention has been presented for purpose of illustration and description. It is not intended to limit the invention to the precise forms disclosed. Many modifications and equivalent arrangements will be apparent.

09680608-400400